APA: Woolcott, O. (2020). Aproximación a cuestiones de responsabilidad civil en la protección de datos personales en Colombia. En O. Woolcot & D. F. Monje-Mayorca (Eds.). *Vicisitudes del derecho a la privacidad (privacy). Cuestiones sobre el tratamiento de datos personales y la responsabilidad civil* (pp. 77-92). Editorial Universidad Católica de Colombia. https://doi.org/10.1471 8/9789585133273.2020.3

Chicago: Woolcott Oyague, Olenka, "Aproximación a cuestiones de responsabilidad civil en la protección de datos personales en Colombia". En *Vicisitudes del derecho a la privacidad (privacy). Cuestiones sobre el tratamiento de datos personales y la responsabilidad civil* editado por Olenka Woolcott Oyague y Diego Fernando Monje Mayorca, 77-92. Bogotá: Editorial Universidad Católica de Colombia. doi: 10.14718/9789585133273.2020.3

PROXIMACIÓN A CUESTIONES DE RESPONSABILIDAD CIVIL EN LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

Olenka Woolcott Oyague

Preliminares

El marco normativo sobre la protección de datos personales en Colombia tiene como punto de partida el reconocimiento constitucional de la intimidad personal que consagra el Artículo 15, es decir, del derecho a la privacidad y a la protección de datos personales, la que a su vez es objeto de la reciente legislación sobre la materia.[115] Como se puede observar en el capítulo precedente, en la actualidad, los sistemas jurídicos se han orientado hacia una legislación especial sobre el tratamiento de datos personales, como una manera de dar respuesta a los nuevos riesgos que surgen con el desarrollo de las tecnologías de la información y que plantean la necesidad de reconocer el nacimiento de un nuevo derecho subjetivo a la protección de los datos personales; es una nueva manifestación en los tiempos actuales del derecho a la intimidad[116] o privacidad del derecho europeo.

Con base en el reconocimiento de una ausencia imputable al Legislador colombiano, al no haber contemplado en el nuevo marco normativo de la protección

115 Se trata de la Ley Estatutaria. Colombia, Congreso de la República, Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales" (Bogotá: *Diario Oficial* núm. 48.587, 18 de octubre de 2012).

116 Ana Herrán Ortiz, *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales (Madrid*: Dykinson, 2002).

de datos el enfoque resarcitorio frente al problema que sugiere la protección de los datos personales, se tratará de identificar en el presente capítulo, a la luz del contexto normativo vigente, las posibilidades que tiene la eventual víctima de los daños derivados de un tratamiento ilícito de datos para obtener un resarcimiento.

Antecedentes normativos en Colombia

El desarrollo del derecho de *habeas data* en Colombia se ha debido fundamentalmente al impulso de la Corte Constitucional, que representa un factor decisivo en el campo de la protección de datos personales, pues a partir de 1992 definió el alcance y las características del derecho, así como las condiciones bajo las cuales se protegen los datos personales, en atención a las pautas internacionales de la ONU.[117]

El Artículo 15 de la Constitución Política de Colombia consagra por primera vez el *habeas data*[118] en los términos siguientes:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.[119]

Como se puede apreciar, cuando la primera parte de la norma consagra el derecho a la intimidad, se refiere también al derecho de *habeas data*, mientras que en la segunda parte se establecen las condiciones bajo las cuales se han de llevar a cabo los tratamientos de datos personales. Al respecto, la Corte Constitucional ha señalado que la segunda parte de la mencionada norma constitucional define el contexto normativo y axiológico dentro del cual debe moverse el proceso

---

117 El *habeas data* es un mecanismo de tutela de la libertad informática y que se asocia a veces con una legislación específica de banco de datos. En América Latina suele tener consagración constitucional. Francisco Zúñiga, "El derecho a la intimidad y sus paradigmas", *Ius et praxis*, núm. 1 (1997): 285-313; Organización de Naciones Unidas [ONU], *Regulación de los archivos de datos personales informatizados, adoptadas mediante Resolución 45/95 de la Asamblea General* (Nueva York, 14 de diciembre de 1990).

118 Para el *habeas data,* Óscar-Raúl Puccinelli, *El habeas data en Indoiberoamérica* (Bogotá: Temis, 1999).

119 República de Colombia, *Constitución Política (Bogotá: Legis, 1991), art.15.*

informático;[120] con ello se ha referido a los principios y las normas que se desprenden del texto constitucional y que deben regir el desarrollo de la informática, y en sus fallos ha acogido los lineamientos de los documentos internacionales de la ONU y la Unión Europea.[121]

El derecho al *habeas data* ha pasado por tres momentos en la interpretación de la Corte Constitucional de Colombia. El primero consideró el *habeas data* como una garantía del derecho a la intimidad y destaca que los datos pertenecen a la vida privada y familiar; el segundo lo contempla como una manifestación del libre desarrollo de la personalidad y sostiene que la autodeterminación y la libertad son fundamentales para el libre desarrollo de la personalidad y el respeto de la dignidad humana; y el tercer momento interpretativo surge a a partir de 1995, al reconocer autonomía al derecho de *habeas data*, cuyo contenido es la autodeterminación informática y la libertad.[122]

No obstante los diversos pronunciamientos de la Corte Constitucional que se refirieron al tratamiento de los datos personales y su protección, así como diversas iniciativas legislativas en esa línea, fue recién en el año 2008 que se sancionó la Ley Estatutaria 1266 de 31 de diciembre, normativa que estuvo circunscrita al sector comercial o financiero, es decir, a los datos que se recolectaran de los titulares de la información por parte de las centrales de riesgos en cuyas bases de datos quedaba almacenada. El objetivo de dicho almacenamiento consistía en la posibilidad de conocer los comportamientos crediticios de los consumidores y clientes financieros, con el propósito de crear un perfil de crédito. La Corte Constitucional aclaró que dicha normativa constituía un régimen parcial y sectorial del derecho de *habeas data*, pues solo era aplicable a los datos personales relativos al cumplimiento o incumplimiento de obligaciones dinerarias.[123]

---

120 Se trata de Colombia, Corte Constitucional, *Sentencia T-307 de 5 de mayo de 1999,* M. P. Eduardo Cifuentes Muñoz; *Sentencia T-414 de 16 de junio de 1992; Sentencia T-729 de 5 de septiembre de 2002,* M. P. Eduardo Montealegre Lynett.

121 En este sentido explica Nelson Remolina-Angarita, *Data protection: panorama nacional e internacional, en Internet, comercio electrónico y telecomunicaciones* (Bogotá: Legis, 2002).

122 En este sentido, "la Corte señaló que el *habeas data* estriba en la defensa del derecho a la autodeterminación informática, en cuya virtud la persona a la cual se refieren los datos que reposan en un archivo público o privado está facultado para autorizar su conservación, uso y circulación". Eduardo Cifuentes, "*El habeas data* en Colombia", *Ius et praxis*, núm. 1 (1997): 81-106.

123 En este sentido, la Sentencia C-1011 de 2008. En esta línea de reafirmación del carácter sectorial de la Ley 1266 de 2008, circunscrito a la protección de la información comercial, crediticia y financiera se pronunció la

Esta normativa, con sus vacíos y críticas insuperables desde la perspectiva de la protección de la información personal y en especial de los llamados datos sensibles,[124] rigió hasta 2012 con el límite de una aplicación sectorial, lo que dejó así el derecho fundamental a la protección de la información personal sin un régimen especial.

El desarrollo galopante que tienen las nuevas tecnologías de la información ha sido un factor decisivo y, quizás también el marco internacional de protección de los datos personales, que rige en Europa y en varios sistemas jurídicos, los hechos que determinaron que el Legislador colombiano optara por extender el campo de protección de los datos allende los límites crediticios y financieros y decidiera la dación de un régimen de protección más amplio y general de los datos personales en Colombia. De allí surgió la Ley Estatutaria 1581 de 2012.

La Ley 1581 de 2012 tiene un marco de disposiciones generales, así como otras disposiciones especiales que regulan los momentos de recolección, manejo y circulación de datos, clasifica los datos según su naturaleza y señala cuáles tienen una especial protección. Además, contempla conductas que se consideran antijurídicas y otras situaciones que pueden eliminar la antijuridicidad de una determinada conducta de manipulación de los datos personales; identifica a los participantes, sus cualidades y funciones en el tratamiento y protección de datos y fija las reglas que permiten velar por la seguridad de la información.

La Ley contempla una definición del dato personal como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables".[125] Sin embargo, entre las sentencias de la Corte Constitucional que antes de la Ley 1581 de 2012 se han referido a los datos personales se encuentra la Sentencia T-414 de 1992, que define que los datos consisten en aquellas informaciones que permiten la identificación de la persona, equiparán-

Superintendencia Financiera en el Concepto 2009029082-002 del 4 de junio de 2009 y la Superintendencia de Industria y Comercio, la cual, en el Oficio 09037876 del 12 de junio de 2009, confirmó el mencionado carácter sectorial de la citada normativa. Nelson Remolina-Angarita, "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?", *International Law, revista colombiana de derecho internacional,* núm. 16 (2010): 489-524.

124 La Ley 1266 de 2012, a diferencia de la normativa internacional, no reguló los datos sensibles, es decir, aquella información que revela el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, sobre la salud y la sexualidad de una persona.

125 Se trata de la Ley 1581 de 2012. Colombia, Congreso de la República, *Ley 1581 de 2012*, art. 3, lit. c.

dose a una "huella digital" por la cual se puede distinguir de otros individuos. En otros términos, se trata de toda información que conduce a identificar a una persona en particular, sus características personalísimas y todo aquello que le concierne.[126]

La Superintendencia de Industria y Comercio, entidad encargada de velar por el cumplimiento de la Ley de protección de datos, ha señalado que "cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación".[127]

La Ley establece dos importantes categorías de datos que exigen una protección especial: la concerniente a los datos sensibles, que afectan la intimidad de las personas o cuyo uso indebido puede dar lugar a discriminación (características personales, datos ideológicos, orientación política, origen, salud, orientación sexual, etc.) y la relativa a los datos de niños, niñas y adolescentes. En sus Artículos 17 y 18 dispone las personas autorizadas para el tratamiento de datos —el responsable y el encargado— lo que tiene relevancia a los fines de la determinación de las obligaciones a cargo de estos sujetos en relación con el titular de los datos, como se explicó en el capítulo anterior referente al régimen italiano y al Reglamento europeo. Por tanto, el suministro de datos personales de manera irresponsable a personas no autorizadas atentaría contra la privacidad y la integridad de la persona, desde que el conjunto de datos relevantes forma parte de la privacidad y la intimidad de la persona. De allí que sea necesaria la normativa de protección de datos personales en cuanto a su circulación, administración, manipulación y tratamiento.

La autorización del titular para el tratamiento de sus datos personales configura el consentimiento y constituye el eje de todo el proceso, según se desprende del Artículo 9 de la Ley 1581 de 2012. Su desarrollo se encuentra en el texto

126 La Corte Constitucional ha señalado como factores distintivos del dato personal que: a) se refiere a aspectos exclusivos y propios de la persona natural; b) facilita la identificación de las personas, sea gracias a la visión de conjunto que se logre con el mismo y otros datos; c) la propiedad es solo del titular de los datos, lo que no se modifica cuando terceros obtienen dichos datos de manera lícita o ilícita; d) su tratamiento se somete a reglas especiales sobre administración y divulgación.
Esta misma sentencia propuso una clasificación de los datos en: a) datos semiprivados; b) datos privados; datos públicos, y d) datos sensibles. Colombia, Corte Constitucional, *Sentencia T-706 de 15 de septiembre de 2014,* M. P. Luis Guillermo Gutiérrez Pérez.

127 Puede verse *Ley Estatutaria 1581 de 2012,* "Por la cual se dictan disposiciones generales para la protección de datos personales" (Bogotá: *Diario Oficial núm. 48.587*, 18 de octubre de 2012).

reglamentario de la Ley Estatutaria, Decreto 1377 de 2013, Capítulo II, Artículos 4 a 12. Aquí pueden surgir dos situaciones: una en la que exista una negativa del titular a suministrar datos, y dos, aquella en la que se produce la ilegalidad de la recolección y del uso posterior, situaciones que pueden desencadenar una responsabilidad civil. La Superintendencia de Industria y Comercio (SIC) se ha referido al consentimiento, al señalar que: "El consentimiento que da cualquier persona para que las empresas o personas responsables del tratamiento de la información, puedan utilizar sus datos personales".[128]

Por su parte, la Corte Constitucional colombiana ha señalado que la autorización para el tratamiento de los datos "debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho […]".[129]

El tratamiento de datos sin autorización constituye un riesgo frente al derecho de autodeterminación, el cual le permite al titular ejercer un control sobre su información personal y con ello representa "un límite para el acopio, procesamiento y transmisión de la información",[130] a fin de que dichos actos se concilien con los derechos fundamentales.

Por su parte, el Reglamento de la ley de protección de datos, Decreto 1377 de 2013, contempló en su Artículo 7 unas conductas inequívocas que llevan a concluir, de forma razonable, que se otorgó la autorización por parte del titular de los datos, por ejemplo, el aviso que se les da a las personas cuando su imagen está siendo tomada por cámaras de seguridad.[131] Sin embargo, este tipo de autorización es susceptible de cuestionamientos ante la ausencia de una manifestación expresa de la voluntad. Si bien podrían existir algunas precisiones normativas, se considera conveniente delegar a la valoración judicial, a la luz de los principios

128 Colombia, Superintendencia de Industria y Comercio, "Cartilla de formatos modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios", https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf (acceso enero 17, 2020).

129 Colombia, Corte Constitucional, *Sentencia SU-082 de 1 de marzo de 1995,* M. P. Jorge Arango Mejía.

130 Alberto Cerda Silva, "Autodeterminación informativa y leyes sobre protección de datos", *Revista chilena de derecho informático,* núm. 3 (2003): 47-75, https://revistas.uchile.cl/index.php/RCHDI/article/view/10661 (acceso enero 30, 2019).

131 Nelson Remolina Angarita, *Tratamiento de datos personales* (Bogotá: Legis, 2013).

consagrados en la misma Ley de protección de datos, la determinación de la calidad o naturaleza del dato personal, su finalidad, etc., en fin, otros criterios que se desprendan de la propia normativa y ayudarán al juez a dilucidar la existencia o no de la autorización mediante la conducta a la que se refiere el Decreto 1377.

La consagración de una reglamentación sobre la autorización para el uso correcto de los datos personales representa una innovación en la normativa sobre protección de datos en Colombia. Con ella se instituye la noción del consentimiento informado como requisito fundamental para el tratamiento de los datos personales, en atención a que los datos pertenecen a su titular y, así, a la esfera de su intimidad.

Si bien el régimen de la Ley Estatutaria 1581 de 2012 es innovadora en el derecho colombiano para proteger intereses de los titulares de datos al control de la información personal, cabe destacar que un importante precedente relativo a los datos en Colombia ha sido la Ley 1266 de 2008, así como sus decretos reglamentarios —Decreto 1727 de 2009 y Decreto 2952 de 2010—, relativa a la recolección y circulación de datos comerciales y financieros con el fin de identificar los riesgos crediticios. Estas normas representan la primera aproximación de la legislación especial de cara a la protección de los datos personales relativos al campo comercial y crediticio y, en este sentido, la primigenia preocupación del Legislador para articular una protección normativa de los datos en Colombia; sin embargo, han sido las nuevas tecnologías de la información las que se convirtieron en el estímulo suficiente para que se dispusiera de una norma que alcanzara la protección de los datos personales allende las fronteras del campo de las relaciones comerciales.

Corresponde reconocer el papel fundamental que desempeñó la jurisprudencia constitucional colombiana sea en la generación o consolidación de las bases actuales para una normatividad sobre la protección de datos. En el primer aspecto cabe citar la Sentencia C-748 de 2011 de la Corte Constitucional, en la cual señaló que el principio de transparencia debia "permitir a cualquier ciudadano establecer con exactitud quiénes son los responsables y encargados del tratamiento de sus datos […]" y la Sentencia T-729 de 2002; en cuanto a consolidar el constructo normativo, se menciona la Sentencia C-1011 de 2008, en la cual se reafirman los conceptos y lineamientos de protección de los datos que introdujo la Ley 1266 de 2008.

Esta breve evolución normativa dio lugar a la Ley Estatutaria 1581 de 2012,[132] que contempló dos categorías de datos que exigen una protección especial y cuyo tratamiento está prohibido. Se trata de los denominados datos sensibles y los datos personales de los niños, niñas y adolescentes. Esta Ley dispuso la creación de la autoridad competente para la protección de datos y prohibió la transferencia de datos a países que carecieran de una protección adecuada.

El Decreto Reglamentario 1377 de 2013 definió el contenido de la autorización y sus alcances, así como el procedimiento de consultas y reclamos que adelanten los titulares. Asimismo, fijó el alcance de la norma en cuanto al derecho de acceso a la información, su rectificación, actualización o modificación (elementos que distinguen el derecho de *habeas data*); dispuso las directivas respecto a los roles y las funciones de los responsables de la información y los encargados de su tratamiento y, por último, determinó que la Delegatura de Protección de Datos de la Superintendencia de Industria y Comercio estaría encargada de la supervisión y del control en materia de datos.

La normatividad de protección de datos personales en Colombia y las cuestiones de responsabilidad civil

Colombia experimenta un avance notorio en la protección de datos,[133] con lo cual trata de adecuarse a los retos que la sociedad de la información pone a los ciudadanos acerca del manejo de la información personal; sin embargo, el Legislador no adoptó una posición en torno al problema de la resarcibilidad de los daños que pueden derivarse de la infracción de las normas de protección de datos y más bien guardó silencio frente a la configuración de un determinado supuesto de responsabilidad. En este sentido, por ejemplo, no se contempla, entre los derechos de los titulares de los datos, el derecho al resarcimiento del daño patrimonial y no patrimonial, circunstancia que explica la ausencia de una referencia expresa al supuesto de responsabilidad que surge con la vulneración de la normativa y la producción de un daño.

[132] Lucero Galvis Cano, "Protección de datos en Colombia avances y retos, *Lebret,* núm. 4 (2012): 195-214, http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336/336 (acceso febrero 7, 2019).

[133] En este sentido, Nelson Remolina-Angarita, "Centrales de información, *habeas data* y protección de datos personales: avances, retos y elementos para su regulación", *Derecho de Internet & Telecomunicaciones* (2012): 358-437.

El Legislador colombiano introdujo una disciplina de carácter predominantemente preventivo y sancionador, conforme se desprende, por un lado, de la previsión sobre los deberes que están a cargo del responsable y de los encargados del tratamiento de datos, de acuerdo con lo contemplado en el Título VI de la Ley 1581 de 2012, Artículos 17 y 18 respectivamente y, por otro lado, de la previsión de los mecanismos de vigilancia y sanción que han sido dispuestos en el Título VII de la misma normativa. Se establece que la Superintendencia de Industria y Comercio por medio de la Delegatura para la Protección de Datos Personales, es la autoridad de protección de datos encargada de la vigilancia en el tratamiento de datos personales, a fin de que se respeten los principios, los derechos, las garantías y los procedimientos estipulados en la Ley y que además adoptará las medidas o impondrá las sanciones correspondientes, de conformidad con el Artículo 22 de la referida Ley.

En esta misma línea, el Decreto 1377 de 2013 reglamenta de manera parcial la Ley 1581 de 2012 y comprende una serie de aspectos entre los cuales cabe destacar, por una parte, la "autorización" requerida para el tratamiento de datos, con lo cual se evidencia la importancia del consentimiento informado ante actos de manipulación de información que pertenece a la esfera privada de la persona. Por otra parte, destaca la incorporación del principio de "responsabilidad demostrada", contenido en el Capítulo VI del mencionado Decreto, con el cual confiere a la Superintendencia de Industria y Comercio la facultad de solicitar a los responsables del tratamiento de datos que demuestren que han implementado las medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y en el Decreto, de una manera proporcional a los criterios que enuncia el propio reglamento, como la naturaleza jurídica del responsable, la naturaleza de los datos personales objeto del tratamiento, el tipo de tratamiento y los riesgos potenciales que puede involucrar el referido tratamiento sobre los derechos de los titulares, de conformidad con el Artículo 26 del mismo Decreto.

La citada normativa pone los "riesgos potenciales que puede causar el tratamiento sobre los derechos de los titulares" como uno de los criterios que permite definir las medidas apropiadas que deben observar los responsables del tratamiento de datos personales, con lo cual se quiere hacer énfasis en el "riesgo" que comporta la actividad y de allí las exigencias comportamentales de la norma respecto a los responsables. Se enuncia también el criterio de la naturaleza jurídica del responsable, es decir, su tamaño empresarial, la naturaleza de los datos personales y el tipo de tratamiento. Como se puede inferir, la exigencia contenida en el régimen vigente de protección de datos sobre las diligencias necesarias por

parte de la SIC, para cumplir con los deberes impuestos por la ley, sí tiene presente el nivel de riesgo que puede comportar el tratamiento de datos en relación con los intereses que pueden resultar vulnerados por esta actividad.

No obstante, el referido Reglamento de la Ley 1581 representa, una vez más, una norma que se sustenta en la función de control y vigilancia del ente administrativo para velar por el cumplimiento de la normatividad de protección de datos. Si bien se hace alusión a una noción de "responsabilidad demostrada", de acuerdo con el citado Reglamento, se trata de una función preventiva, con el propósito de vigilar el cumplimiento de las obligaciones a cargo de los responsables y encargados del tratamiento de datos personales. Por ende, el presente instituto no ha sido pensado para cumplir una función reparadora de los eventuales daños que se pudieran derivar del tratamiento de datos.

La visión del Legislador colombiano, estrictamente preventiva y sancionadora, se afianza con lo dispuesto en el propio texto normativo. Desde una perspectiva punitiva, la Ley introduce en el Artículo 24 una serie de criterios que permiten que la autoridad de protección de datos gradúe las sanciones. Estos criterios, aplicables a cada caso, son los siguientes:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;
b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;
c) La reincidencia en la comisión de la infracción;
d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;
e) La renuencia o desacato a cumplir órdenes impartidas por la Superintendencia de Industria y Comercio;
f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.[134]

Como se puede apreciar, en los criterios que enlista el Legislador se tuvo presente la posibilidad de producirse un daño o de poner en peligro intereses jurídicos tutelados por la Ley, lo que se toma en cuenta solo y únicamente a los fines de imponer una sanción, circunstancia que delata, una vez más, la mirada estrictamente preventiva y punitiva de la ley.

134 Congreso de la República de Colombia, *Ley 1581 de 2012,* art. 24.

Desde esta mirada, el Legislador colombiano no prestó atención alguna a la reparación del daño en el marco de la legislación especial, en el sentido de configurar un supuesto *ad hoc* de responsabilidad civil por tratamiento de datos personales.

En otros términos, el Legislador no desconoce de la posibilidad de que se ocasionen daños por el tratamiento ilícito de los datos personales, pero desatiende por completo el problema resarcitorio, al no dedicarle la atención necesaria en el plano de la legislación especial, más aún si se tiene presente que el aspecto resarcitorio es inescindible de la prevención de los riesgos de daños por tratamiento ilícito de datos personales, como se evidencia en el plano de la normatividad internacional que se ocupa del problema.

En efecto, en el primer capítulo de este libro se observó que el Legislador europeo sí aborda el problema resarcitorio de los daños derivados de un tratamiento ilícito de datos personales por medio de la previsión de un supuesto especial de responsabilidad civil, para el cual parte de la existencia de un riesgo inherente que implica el tratamiento de datos personales y, en virtud de ello, opta por apartarse de la regla tradicional de la responsabilidad por culpa en la imputación de la responsabilidad, de lo que resulta un aligeramiento de la carga probatoria para la eventual víctima de estos daños.

La ausencia del mecanismo resarcitorio en el marco de una normativa de protección de datos personales delata que la ley colombiana es una normativa con una visión parcial del problema de la protección de datos, observación que se agrega a las críticas que tuvo en su momento la referida Ley Estatutaria 1581 de 2012, toda vez que se cuestiona —incluso desde la propia perspectiva preventiva y sancionadora, que es la esencia de dicha ley— que no contenga los mecanismos que obliguen a las empresas que administran bases de datos personales a contactar sus clientes, con el fin de obtener su autorización para el respectivo tratamiento, con lo cual se facilita el camino a la vulneración de la intimidad de las personas.[135]

[135] En este sentido, Virginia Vega Clemente, "Comercio electrónico y protección de datos", *Revista de estudios económicos y empresariales,* núm. 25 (2013): 205-244. En cuanto a señalar la inseguridad de los datos en el mercado, Álvaro de Angulo Sanz y Luz Ángela Duarte González, "*Habeas data* y dirección IP: un mercado potencialmente inseguro para los datos personales" (Tesis de Maestría, Pontificia Universidad Javeriana de Bogotá, 2015). Al respecto, la propia Corte Constitucional de Colombia se ha pronunciado sobre la insuficiencia de la Ley 1581 de 2012 en relación con la protección de los datos personales de consumidores de comercio electrónico y señaló que el texto normativo "da lugar a profundas dificultades interpretativas y, en general, a una injustificada disminución del ámbito de protección del derecho al *habeas data*". Salvamento de voto recaído en Colombia, Corte Constitucional, *Sentencia C-748 de 6 de octubre de 2011,* M. P. María Victoria Calle Correa, Jorge Iván Palacio y Luis Ernesto Vargas Silva.

Ante el silencio del Legislador colombiano sobre un tema fundamental para consolidar una adecuada protección del interesado en la protección de sus datos personales como es la perspectiva resarcitoria de los daños, se puede inferir que aquel no comparte la posición del régimen de protección que consagra la normativa europea, así como el reciente Reglamento de protección de datos personales en Europa (RPDP) o la concreta experiencia italiana que se ha tomado como base en el presente libro, con el propósito de poner en evidencia el vacío de la normativa colombiana.

En este sentido, el Legislador colombiano optó por una delegación tácita a los jueces de toda cuestión de responsabilidad civil por daños derivados de tratamiento ilícito de los datos personales, es decir, los jueces tienen la tarea de delinear y seleccionar los criterios para la valoración de la conducta generadora de un daño derivado de un tratamiento ilícito de los datos personales, de manera que los casos de daños que se presenten quedan librados a la aplicación del régimen de responsabilidad civil consagrado en el Código Civil colombiano. En otros términos, al guardar silencio sobre la reparación de los daños por tratamiento de datos personales, el Legislador colombiano se conformó con que el actual régimen general de la responsabilidad civil sea, en realidad, la única base normativa con la cual los jueces puedan hacer frente a los casos que planteen un eventual resarcimiento de daños en el campo que ocupa el interés de este libro, profundamente permeado además por el influjo de las nuevas tecnologías de la información.

Si bien el Reglamento de la Ley Estatutaria, Decreto 1377 de 2013, parecería aproximarse al problema de la responsabilidad, al mencionar en el Artículo 26 los "riesgos potenciales" que el tratamiento puede causar sobre los derechos de los titulares, se puede colegir que tal alusión no apunta a la determinación del daño para los fines de su resarcimiento, sino solo para determinar las medidas apropiadas y efectivas que deben adoptar los responsables del tratamiento de datos personales para cumplir con las obligaciones instituidas por la ley; con ello, el texto pone de manifiesto el carácter administrativo de la responsabilidad en la que incurriría el responsable del tratamiento, de no aportar la prueba de la diligencia solicitada por la SIC. En suma, el Legislador colombiano no contempló una especial solución indemnizatoria para los casos de daños que se generen por el tratamiento de datos.

El Legislador colombiano delegó al juez la eventual tarea de una determinación del supuesto de responsabilidad por daños derivados de un tratamiento ilícito de datos personales. Se trata de una labor compleja, pues el juez tendrá que poner a prueba el régimen vigente de la responsabilidad civil en un contexto novedoso: el tratamiento de datos personales a cargo de sujetos que actúan normalmente en el comercio, donde la tecnología facilita la circulación de la información en dimensiones no imaginadas para el derecho tradicional de la responsabilidad civil. El juez tendrá en su haber el recurso a la cláusula general de la responsabilidad por culpa, contemplado en el Artículo 2341 del Código Civil, con las dificultades de aplicación para un caso de las características que presenta el problema de los datos personales y la circulación por medios tecnológicos y la no menos pacífica vía que propone la aplicación del supuesto del Artículo 2356 del mismo cuerpo legal, la cual, al consagrar el supuesto de la responsabilidad por riesgo, pareciera conciliarse con la naturaleza "inherentemente" riesgosa de la actividad de tratamiento de datos.

Ante el vacío de la legislación especial del tratamiento de datos personales y a la luz de las propuestas que surgen en el derecho europeo, con especial atención a que el desarrollo actual del tratamiento de datos surge por la herramienta tecnológica, se propone que los eventuales problemas de daños que puedan surgir con el tratamiento ilícito de datos personales sean pensados a partir del énfasis en el riesgo de la mencionada actividad, lo que permitirá dar forma, por la vía jurisprudencial, a un nuevo supuesto de responsabilidad civil, que exija la aplicación del régimen de responsabilidad objetiva por riesgo. De ser esta la opción de la jurisprudencia, orientación que prevalece en el enfoque del Legislador europeo, como se ha visto en el primer capítulo, se abordará en el capítulo sexto, el problema de la responsabilidad civil en el caso de tratamiento de datos personales quedaría como uno más de los tantos que, al reportar un riesgo inherente, se somete a las arenas movedizas que han caracterizado las soluciones indemnizatorias en Colombia, a la luz de la aplicación del Artículo 2356 del Código Civil.[136]

Consideraciones conclusivas

Si se parte de que las sociedades actuales requieren una efectiva protección de los datos personales para la consecución de los fines democráticos y el

[136] Para una explicación jurisprudencial del desarrollo que ha tenido el Artículo 2356 del Código Civil colombiano y la mirada al derecho comparado, puede verse Woolcott et al., *Estudios contemporáneos.*

desenvolvimiento normal de la personalidad de los conciudadanos,[137] en atención a los nuevos riesgos de exposición al peligro que acechan la intimidad de las personas y su desarrollo normal en un marco de consagración de los derechos fundamentales, se puede concluir que el esquema de protección europeo es un referente garantista en cuanto a la protección internacional de los datos personales, que contempla no solo la perspectiva de protección preventiva y sancionadora, sino que, en línea a una efectiva tutela de los datos personales, comprende la perspectiva resarcitoria de los daños, sin cuya consideración la protección de los datos personales deviene incompleta.

Si bien Colombia ha hecho esfuerzos orientados a la protección de los datos personales,[138] lo que se observa en la legislación y la jurisprudencia de la Corte Constitucional, que incluso precedió a la dación de la normatividad vigente, cabe llamar la atención sobre la ausencia, en la actualidad, de una clara y adecuada posición frente al problema resarcitorio de los daños que puedan surgir —y, sin duda, surgen— de un tratamiento ilícito de los datos personales.

En este sentido, en Colombia existe una normatividad que consagra los derechos y las obligaciones que se desprenden del derecho a la protección de los datos personales, unas medidas de prevención y otras punitivas para el caso de infracción normativa. Existe una entidad —la Superintendencia de Industria y Comercio— que tiene una delegatura destinada a la protección de los datos personales y ejerce un control de eminente carácter administrativo, para canalizar la protección preventiva y sancionadora en relación con los datos personales. Se reitera: queda siempre al descubierto la no finalidad resarcitoria de la protección, función que, por ausencia de régimen expreso, se entiende delegada al juzgador, quien, a la luz del régimen tradicional de la responsabilidad civil, debe intentar una reconstrucción de los supuestos de responsabilidad ante la eventualidad de los daños que se deriven de un tratamiento ilícito de los datos personales.

En el sistema jurídico italiano, tomado como un caso paradigmático para el estudio de la protección de datos personales en Europa, ha sido la jurisprudencia la que ha afrontado el problema del resarcimiento del daño por infracción de la normativa de datos personales, con énfasis en el terreno del daño no patrimonial.

137 Así, Stefano Rodotà, "Democracia y protección de datos", *Cuadernos de derecho público,* núm. 19-20 (2003): 15-26.

138 Así, Marcela Rojas Bejarano, "Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales", *Novum Jus 8,* núm. 1 (enero-junio 2014): 107-139.

Aquí surge una variedad de posturas y criterios para tratar de determinar la existencia de un daño no patrimonial resarcible, a la luz de la propia normativa de protección de datos que consagra expresamente un supuesto de responsabilidad civil especial, si se toma como referente el régimen general de la responsabilidad civil consagrada en el Código Civil. Prevalece la postura de la resarcibilidad del daño no patrimonial por violación de los derechos de la personalidad, considerados en su acepción tradicional y tutelados incluso fuera de la normativa de protección de datos por el propio orden constitucional. Las dificultades se presentan, de manera particular, en la determinación de la existencia del daño patrimonial cuando la norma de protección de datos personales que ha sido violada no concierne a un interés directo del titular de los datos, sino a un interés más general, como es el derecho a controlar la circulación de los datos.

En el derecho italiano, el Artículo 15 del Decreto 196 de 2003, régimen vigente de protección de datos personales, contempló las consecuencias resarcitorias del ilícito tratamiento de datos personales y así prevé de manera puntual la reparación del daño patrimonial y del daño no patrimonial. El régimen hace una remisión expresa al Artículo 2050 del Código Civil, circunstancia que desencadenó unas discusiones interminables en torno a su aplicación. En efecto, la citada norma se inserta entre los supuestos de responsabilidad agravada, en los que se atribuye la responsabilidad a quien realice una actividad riesgosa y solo puede exonerarse con la prueba de toda medida destinada a evitar el daño. Para esta norma de responsabilidad, la prueba de la causal exoneratoria no sería la prueba de la ausencia de culpa la que, por excepción, gravaría negativamente sobre el dañante en lugar que positivamente sobre la víctima, sino que sería la prueba de que la conducta peligrosa del agente dañante no tendría conexión alguna con el daño sufrido por la víctima. De esta manera, la prueba que corresponde invocar y probar, en el marco del Artículo 2050 del Código Civil, es el de una ruptura causal. Sin embargo, según otra posición, la prueba exoneratoria de la responsabilidad consistiría en acreditar la ausencia de culpa, al probar que se hizo todo lo posible para impedir el daño y que se respetaron todas las normas de la diligencia calificada, de acuerdo con la peligrosidad o naturaleza de la actividad.

De esta manera, la doctrina italiana pone en evidencia dos posturas que se refieren a la prueba liberatoria de la responsabilidad: por una parte, la ruptura de

la relación causal y, por otra, una postura que sostiene una responsabilidad semi agravada que no es del todo una responsabilidad objetiva.

La jurisprudencia italiana presenta una dualidad de corrientes en materia del resarcimiento del daño por vulneración de la normativa de protección de datos personales: una corriente jurisprudencial que asume la tesis del daño *in re ipsa* que no ha sido del todo superada y es seguida aún por las Cortes de mérito y otra corriente que se va perfilando como prevalente, contrapuesta a la precedente, que exige concurrencia de la prueba de un daño-consecuencia, el cual se deriva de la ilegítima señalación por la central de riesgo;[139] tal orientación es la asumida por la sentencia de 2017 que resuelve el caso cuyo examen se reporta en el anterior capítulo, con el cual se trata de ilustrar la dimensión del problema resarcitorio del daño no patrimonial que se presenta para el derecho italiano con ocasión de un tratamiento ilícito de datos personales por una central de riesgos.

Esta misma línea de orientación jurisprudencial en Italia pone de relieve la necesaria distinción entre el daño-evento y el daño-consecuencia sobre el que se estructura el resarcimiento del daño en el sistema jurídico de ese país.[140] Sostener que la sola conducta que vulnera la normativa de protección de datos personales encierra en sí misma un daño resarcible supondría reconocer que el resarcimiento se concede no como resultado de la verificación de un daño, sino a título de una pena privada por la conducta antijurídica,[141] cuando la naturaleza del resarcimiento es compensatoria y no simplemente punitiva.

A todo ello cabe agregar que, en la materia de tratamiento ilícito de datos personales, la resarcibilidad del daño se sujeta, además, a la valoración por el juez de un límite mínimo de gravedad de la lesión y seriedad del daño como pérdida de naturaleza personal que ha sido realmente padecida por el interesado, de modo que no basta la sola lesión del derecho fundamental a la protección de los datos personales, de acuerdo con el Artículo 11 del Código de la Privacidad, sino que es necesario que la lesión ofenda de manera sensible el derecho del interesado.

139 Ponzanelli, "Il problema", 1092-2004; Ziviz, "La fallacia", 1720-1726.

140 Procida Mirabelli Di Lauro, "Il danno", 219-264; Emanuela Navarretta, "Ripensare", 1-26; Franzoni, *Dei fatti,* 1170.

141 Bonilini, "Pena privata", 159-174; Francesco Busnelli, "Verso una riscoperta delle pene private?", *Responsabilità civile e previdenza* (1984): 26-35.